* NOTICES *

Machine Translation of JP 11-298470



1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

## DETAILED DESCRIPTION

[Detailed Description of the Invention]
[0001]
[Field of the Invention] This invention relates to the technology of distributing the key used for cryptocommunication to a key user (for example, addressee of code data).
[0002]
[Description of the Prior Art] Generally, when carrying out cryptocommunication of a lot of data, the secret key cryptosystem is used. It is necessary to have a common key (common key) between a transmitting person and an addressee in a secret key cryptosystem. As the delivery method of a common key, although there are a copy key method, an individual key method, etc., in the case of which, private key information must be distributed to an addressee. Conventionally, private key information was carried in the IC card etc., an addressee is supplied widely off-line, or it is transmitting private key information to an addressee by cryptocommunication etc., and private key information is distributed to the addressee.
[0003]
[Problem(s) to be Solved by the Invention] However, by the method of carrying private key information in an IC card etc., and distributing off-line, an inaccurate person uses this storage by stealth, and a possibility of becoming the addressee of normal and clearing up can be considered. Moreover, by the method of transmitting private key information by cryptocommunication etc., an inaccurate person intercepts and decodes private key information, and a possibility of becoming the addressee of normal and clearing up can be considered.
[0004] This invention is made in view of the above-mentioned situation, and in case the purpose of this invention distributes private key information, the private key information concerned decreases a possibility of being seized by the inaccurate person, and is to raise the security of cryptocommunication.
[0005]
[Means for Solving the Problem] In order to solve the above-mentioned technical problem, this invention is the distribution method of a key used for cryptocommunication, and is set to a key manager's equipment. The 1st step which creates a private key S and divides the private key S concerned into at least two confidential information S1-Sn (n>=2), In the 2nd step which distributes off-line at least one confidential information Si among the confidential information S1-Sn obtained at said 1st step (1 <=i<=n) to a key user, and a key user's equipment The confidential information Si

distributed off-line by said 2nd step In the 3rd step which creates the authentication information AS and transmits the authentication information AS concerned to a key manager's equipment based on the identification information ID beforehand given by key manager, and a key manager's equipment The 4th step which performs authentication processing of a key user based on the authentication information AS transmitted by said 3rd step, When a key user is attested at said 4th step, to equipment of the key user concerned In the 5th step which transmits confidential information other than the confidential information Si distributed to the key user concerned off-line at said 2nd step among the confidential information S1-Sn obtained at said 1st step, and a key user's equipment It is characterized by having confidential information S1-Sn other than confidential information Si transmitted by said 5th step, and the 6th step which creates said private key S based on the confidential information Si distributed off-line by said 2nd step.

[0006] According to this invention, a key manager divided a private key S into two or more confidential information S1-Sn, carried at least one of the confidential information [ them ] Si in a storage (storages with a count function, such as an IC card, are included), and has supplied a key user widely off-line. And only when a key user is attested using the authentication information AS created based on the identification information ID given to confidential information Si and a key user, he is trying to transmit to the key user concerned on-line about the remainder.

[0007] thus -- even if a storage distributed off-line is used by stealth for an inaccurate person by carrying out -- so much -- coming out -- it does not mean that an inaccurate person had acquired all the confidential information S1-Sn required to restore a private key S Even if similarly confidential information which transmitted on-line is intercepted by inaccurate person, it does not mean that an inaccurate person had acquired all the confidential information S1-Sn required to restore a private key S only by it. For this reason, in case private key information is distributed, a possibility that the private key information concerned will be seized by inaccurate person can be decreased, as a result security of cryptocommunication can be raised.

[0008] In addition, when, as for the 5th step, a key user is attested at the 4th step in this invention, Inside of the confidential information S1-Sn obtained at said 1st step to equipment of the key user concerned, It is what enciphers said confidential information Si to the key user concerned as a key, and transmits confidential information other than the confidential information Si distributed off-line to him at said 2nd step. The 6th step Said confidential information Si may be decrypted for the confidential information S1-Sn which was transmitted by the 5th step and as which it was enciphered other than confidential information Si as a key, and said private key S may be created based on a decode result and said confidential information Si.

[0009] By doing in this way, security at the time of transmitting confidential information S1-Sn other than confidential information Si on-line can be raised further.

[0010]

[Embodiment of the Invention] Below, 1 operation gestalt of this invention is explained.

[0011] Drawing 1 is the schematic diagram of the system by which the private key distribution method which is 1 operation gestalt of this invention was applied.

[0012] This operation gestalt method is enforced in the system constituted by the key manager equipment 100 and the key user equipment 200 which were mutually connected by the communication line 400, and key manager equipment 100 and key user equipment 200 including the storage 300 with a count function constituted possible [ insert and remove ] so that it may illustrate.

[0013] The outline functional configuration of key manager equipment 100 is shown in drawing 2 .
[0014] key manager equipment 100 comes out with the random-digits generation section 101, operation part 102, the dark decryption section 103, the authentication section 104, the accounting section 105, memory 106, and the communications department 107, and is constituted so that it may illustrate. In a computer, it may realize by software and these functional configurations may be made to realize by constructing the logic which realizes each function by executing the program the procedure for realizing each function was described to be in hardware. When realizing by software, the program the procedure for realizing each function was described to be is stored in storages, such as CD-ROM, and you may make it supply it to a computer.
[0015] In addition, the device for connecting to key manager equipment 100 the storage 300 with a count function distributed to a key user off-line is established.
[0016] The outline functional configuration of key user equipment 200 is shown in drawing 3 .
[0017] key user equipment 200 comes out with the random-digits generation section 201, the prime-number-generation section 202, operation part 203, the dark decryption section 204, memory 205, and the communications department 206, and is constituted so that it may illustrate. Like key manager equipment 100, it may realize by software and these functional configurations may be made to realize by constructing the logic which realizes each function by executing the program the procedure was described to be in hardware, in order to realize each function in a computer. When realizing by software, the program the procedure for realizing each function was described to be is stored in storages, such as CD-ROM, and you may make it supply it to a computer.
[0018] In addition, the device for key user equipment 200 to connect the storage 300 with a count function distributed by the key manager off-line is established.
[0019] The outline functional configuration of the storage 300 with a count function is shown in drawing 4 .
[0020] the storage 300 with a count function comes out with the dark decryption section 301, operation part 302, and memory 303, and is constituted so that it may illustrate. In an IC card, it may realize by software and these functional configurations may be made to realize by constructing the logic which realizes each function by performing the program the procedure was described to be in hardware, in order to realize each function.
[0021] Next, the private key distribution method which is enforced in the system which gave [ above-mentioned ] explanation and which is the first operation gestalt of this invention is explained.
[0022] First, according to directions of a key manager, by the random-digits generation section 101, key manager equipment 100 generates random digits S, and makes this a key user's private key. Then, operation part 102 divides a private key S into confidential information S1 and S2, and a private key S and confidential information S1 and S2 are stored in memory 106. Next, key manager equipment 100 is stored in the memory 303 in the storage 300 with a count function by which confidential information S1 was connected to ejection from memory 106, and, as for it, this was connected to key manager equipment 100.
[0023] A key manager distributes off-line the storage 300 with a count function with which confidential information S1 was stored to the target key user.
[0024] The key user who received the storage 300 with a count function with which confidential information S1 was stored connects this to key user equipment 200.
[0025] Key user equipment 200 performs authentication processing between key manager equipment

100 using the identification information ID of the key user concerned to which confidential information S1 was beforehand given by ejection, confidential information S1, and the key manager according to directions of a key user from the storage 300 with a count function.

[0026] Although there are various methods in authentication processing, the case where the case where the RSA signing method is used, and the ERUGAMARU signing method are used as an example is explained here.

[0027] First, the case where the RSA signing method is used is explained.

[0028] According to directions of a key user, beforehand, key user equipment 200 creates the following information using the random-digits generation section 201, the prime-number-generation section 202, and operation part 203, and stores it in memory 205.

[0029]

[Equation 1]

数1

- 秘密情報　　$p,q$：素数
- 署名鍵　　$(d,n), d \in \mathbb{Z}, n=pq$
- 検証鍵　　$(e,n), e \in \mathbb{Z}, n=pq$　　・・・(数1)

[0030] Here, a signature key considers a secret and a verification key as public presentation. Key user equipment 200 outputs the identification information ID of the key user concerned beforehand given by the key manager whom the key user inputted as the signature key to the storage 300 with a count function. In response, the storage 300 with a count function is [0031] by operation part 302.

[Equation 2]

数2

$$AS = S'^{d} \pmod{n} \qquad \cdots(数2)$$

[0032] since -- the authentication information AS is calculated. Here, S' is the predetermined value of a function (for example, hash value) which considers confidential information S1 and identification information ID as an input. Next, the storage 300 with a count function outputs the authentication information AS to key user equipment 200. In response, key user equipment 200 transmits the authentication information AS to key manager equipment 100 through a communication line 400 by the communications department 206.

[0033] Key manager equipment 100 is [0034] by the authentication section 104, when the communications department 107 receives the authentication information AS.

[Equation 3]

数3

$$S' = AS^{e} \pmod{n} \qquad \cdots(数3)$$

[0035] It verifies whether it ****** or not, and if materialized, the key user of key user equipment 200 who has sent the authentication information AS will attest with his being a just key user. In addition, key manager equipment 100 shall be matched with the confidential information S1 stored in the storage 300 with a count function which distributed off-line the identification information ID

given to the key user to the key user concerned, and shall be stored in memory 106.
[0036] Next, the case where the ERUGAMARU signing method is used is explained.
[0037] According to directions of a key user, key user equipment 200 generates the prime factor p by the prime-number-generation section 202, and is [0038] by operation part 202.
[Equation 4]
数4

$$\mathrm{ord}_p(\alpha)=p-1 \qquad \cdots(数4)$$

[0039] ******** alpha is created. And alpha and the prime factor p which were created are outputted to the storage 300 with a count function. In response, the storage 300 with a count function is [0040] by operation part 302.
[Equation 5]
数5

$$y=\alpha^{S'} \pmod p \qquad \cdots(数5)$$

[0041] ******** y is calculated and x, (alpha, p), and a verification key are set to (y, alpha, p) for a signature key. Here, S' is the predetermined value of a function (for example, hash value) which considers confidential information S1 and identification information ID as an input.
[0042] Next, key user equipment 200 creates p-1 and the relatively prime random digits k by the random-digits generation section 201, and is [0043].
[Equation 6]
数6

$$r=a^k \pmod p \qquad \cdots(数6)$$

[0044] ******** r is calculated. Furthermore, the random-digits generation section 201 generates the suitable message m, and it outputs to the storage 300 with a count function with r and k. In response, the storage 300 with a count function is [0045] by operation part 302.
[Equation 7]
数7

$$\mathrm{t}=(m-S'r)k^{-1} \pmod{p-1} \qquad \cdots(数7)$$

[0046] ******** t is calculated. And (r, t) are considered as the signature to Message m, and Message m and a signature (r, s) are outputted to key user equipment 200. In response, key user equipment 200 transmits Message m and a signature (r, s) to key manager equipment 100 through a communication line 400 from the communications department 206.
[0047] Key manager equipment 100 is [0048] by the authentication section 104, when Message m and a signature (r, s) are received.
[Equation 8]
数8

$$\alpha^m=y^r r^t \pmod p \qquad \cdots(数8)$$

[0049] It verifies whether it ****** or not, and if materialized, the key user of key user equipment 200 who has sent Message m and the signature (r, s) will attest with his being a just key user. In addition, key manager equipment 100 shall be matched with the confidential information S1 stored in the storage 300 with a count function which distributed off-line the identification information ID given to the key user to the key user concerned, and shall be stored in memory 106.
[0050] If a key user is attested by the authentication processing explained above, key manager equipment 100 will encipher confidential information S2 by using confidential information S1 as a key by the dark decryption section 103. And the enciphered confidential information S2 is transmitted to key user equipment 200 through a communication line 400 by the communications department 107.
[0051] Key user equipment 200 will output this to the storage 300 with a count function, if the enciphered confidential information S2 is received. In response, by the dark decryption section 301, the storage 300 with a count function decrypts confidential information S1 as a key, and stores the enciphered confidential information S2 in memory 303. Furthermore, with an arithmetic unit 302, based on the decrypted confidential information S2 and confidential information S1, a private key S is restored and it stores in memory 303.
[0052] Next, key user equipment 200 performs authentication processing for a private key S with the same procedure as the above between key manager equipment 100 using ejection and this private key S according to directions of a key user from the storage 300 with a count function.
[0053] In addition, what is necessary is just to use a private key S instead of S' in above (several 2) and (several 3), when using the RSA signing method. Moreover, what is necessary is just to use a private key S instead of S' in above (several 5) and (several 7), in using the ERUGAMARU signing method.
[0054] If a key user is attested, by the accounting section 105, key manager equipment 100 generates the registration tariff information (accounting information) over the cryptocommunication which used the private key S of the key user concerned, and stores this in memory 106. This information is used on the occasion of billing to the key user concerned.
[0055] By the above-mentioned processing, if a private key S is distributed to a key user, a key user will perform cryptocommunication among information providers using a private key S. Or after doing key sharing among information providers using a private key S, the share key performs cryptocommunication.
[0056] Here, the system for performing cryptocommunication between a key user when a key manager and an information provider are the same, and an information provider is shown to drawing 5 . Information provider equipment 500 performs cryptocommunication between the key user equipment 200 of the key user concerned using the private key S distributed to the key user with key manager equipment 100 so that it may illustrate.
[0057] With this operation gestalt, the key manager divided the private key S into confidential information S1 and S2, carried confidential information S1 in the storage (storages with a count function, such as an IC card, are included), and has supplied the key user widely off-line. And only when a key user is attested using the authentication information AS created based on the identification information ID given to confidential information S1 and a key user, he is trying to transmit to the key user concerned on-line about confidential information S2.
[0058] thus -- even if the storage distributed off-line is used by stealth for an inaccurate person by carrying out -- so much -- coming out -- an inaccurate person can acquire no confidential information

S1 and S2 required to restore a private key S. For this reason, in case private key information is distributed, a possibility that the private key information concerned will be seized by the inaccurate person can be decreased, as a result the security of cryptocommunication can be raised.

[0059] In this operation gestalt moreover, key manager equipment 100 When a key user is attested by the authentication information AS created based on the identification information ID given to confidential information S1 and a key user, Confidential information S1 was enciphered to key user equipment 200 as a key, confidential information S2 was transmitted to it, and key user equipment 200 decrypted confidential information S1 for the enciphered confidential information S2 as a key, and has restored the private key S based on a decode result and confidential information S1. By doing in this way, the security at the time of transmitting confidential information S2 on-line can be raised further.

[0060] In addition, the above-mentioned operation gestalt explained the case where a private key S was divided into two confidential information S1 and S2. However, this invention is not limited to this and you may make it divide a private key S into at least two confidential information S1-Sn. In this case, what is necessary is to distribute at least one of them off-line, and just to transmit the remainder on-line using a communication line.

[0061] Moreover, although the above-mentioned operation gestalt explained what stored accounting information in the memory 106 in key manager equipment 100 by the accounting section 105 of key manager equipment 100, this invention is not limited to this. For example, instead of forming the accounting section 105 in key manager equipment 100, it prepares in key user equipment 200 or the storage 300 with a count function, and you may make it store accounting information in the memory 205 in key user equipment 200, or the memory 303 in the storage 300 with a count function. This information is sucked up and used for key manager equipment 100 on the occasion of billing to a key user.

[0062]

[Effect of the Invention] As explained above, in case a key manager distributes private key information to a key user according to this invention, a possibility that the private key information concerned will be seized by the inaccurate person can be decreased, as a result the security of cryptocommunication can be raised.

---

[Translation done.]